OpenChirp: A Low-Power Wide-Area Networking Architecture

Adwait Dongare[‡], Craig Hesling[‡], Khushboo Bhatia[‡], Artur Balanuta[‡][†],
Ricardo Lopes Pereira[†], Bob Iannucci[*] and Anthony Rowe[‡]
[‡]Electrical and Computer Engineering Department, Carnegie Mellon University, Pittsburgh, USA
[†]Instituto Superior Técnico, University of Lisbon, Lisbon, Portugal
[*]Electrical and Computer Engineering Department, Carnegie Mellon University - Silicon Valley, Mountain View, USA

***Abstract*—*Infrastructure monitoring* applications currently lack a cost-effective and reliable solution for supporting the last communication hop for low-power devices. The use of cellular infrastructure requires contracts and complex radios that are often too power hungry and cost prohibitive for sensing applications that require just a few bits of data each day. New low-power, sub-GHz, unlicensed band long-range radios are an ideal technology to help fill this communication void by providing access points that are able to cover multiple kilometers of urban space with thousands of end-point devices. These new Low-Power Wide-Area Networking (LPWAN) platforms provide a cost-effective and highly deployable option that could piggyback off of existing public and private wireless networks (WiFi, Cellular, etc).**

In this paper, we present OpenChirp, a prototype end-to-end LPWAN architecture built using LoRa Wide-Area Network (LoRaWAN) protocol with the goal of simplifying the design and deployment of Internet-of-Things (IoT) devices across campuses and cities. We present a software architecture that exposes an application layer allowing users to register devices, describe transducer properties, transfer data and retrieve historical values. We define a service model on top of LoRaWAN that acts as a session layer to provide basic encoding and syntax to raw data streams. At the device-level, we introduce and benchmark the open-source LoRaBug hardware platform. It is a LoRa client that can be extended with custom transducers, and can also interact with Bluetooth Low-Energy (BLE) devices. We evaluate the system in terms of end-node energy consumption, radio penetration into buildings as well as coverage provided by a network currently deployed at Carnegie Mellon University.

I. INTRODUCTION

Low-power, low-cost and pervasive telemetry still remains a bottleneck in how we sense and manage our physical infrastructure. Taking Internet-of-Things (IoT) concepts outside of buildings and to massive scales will have deep implications for monitoring utilities (water, electricity, gas), sewage, roads, traffic lights, bridges, parking complexes, agriculture and waterways. Current approaches for telemetry rely on cellular infrastructure or nearby WiFi that were optimized for high-throughput applications. In terms of energy, cost and scalability per bit of information, these existing radios will not be able to support long-term deployments of battery operated sensing devices. Fortunately, the same radio technology that has resulted from advances in WiFi, Bluetooth and LTE have now made it possible to create new chipsets that trade-off throughput for range. These Low-Power Wide Area Networking (LPWAN) radios are able to transmit over distances as long as 10 km with the same power consumption (or less) than what is used by typical WiFi radios. They also operate at lower frequencies (below 1 GHz) that are able to penetrate more deeply into structures. These radios use the ISM bands (433/915 MHz in the U.S. and similar frequencies elsewhere), which means no licensing is required for public access.

In this paper, we discuss early progress towards an open source LPWAN infrastructure called OpenChirp. OpenChirp is designed to allow multiple users and groups the ability to provision and manage battery-operated transducers across large facilities like campuses, manufacturing plants or cities. The system is built using LoRa (short for *Long Range*) radios which are an LPWAN technology developed by Semtech. Each radio transmits data using a form of Chirp Spread Spectrum (CSS) over a narrowband (125 KHz or 500 KHz) channel in the 433 MHz and 915 MHz ISM bands. Data rates can be varied between 0.3 kbps to 22 kbps by adjusting packet spreading factors, bandwidth and power levels.

A unique aspects of LoRa systems is that the gateway chipsets can demodulate on multiple channels and at multiple data rates simultaneously. This enables LoRa gateways to support extremely efficient star collection topologies. In an analogy to the OSI communication stack, LoRa radios define the first and second layers (Physical and Data Link) of LPWAN. Layers three and four (Network and Transport) are analogous to the LoRa Wide-Area Network (LoRaWAN) protocol. LoRaWAN is an openly defined network protocol that manages communication between gateways and end-devices with the following features: (1) establishing encryption keys for application payloads and network traffic, (2) device to gateway pairing assignments, and (3) channel, power and data rate selection. LoRaWAN defines three main device classes: bi-directional end-devices with downlink followed by uplink (Class A), bi-directional end-devices with transmission slots scheduled for downlink (Class B) and always-on bi-directional devices (Class C). Class A is primarily intended for sensors, Class B is intended for sensors with actuators while Class C is intended for powered devices that require low-latency. Each LoRa device in the system has a network communication and application encryption key. All packets are transparently sent from gateways to a LoRaWAN server without any local decryption to limit the potential risk of compromised clients and gateways. Since packet decoding and MAC parameters like data-rate and power-level are decided at the LoRaWAN

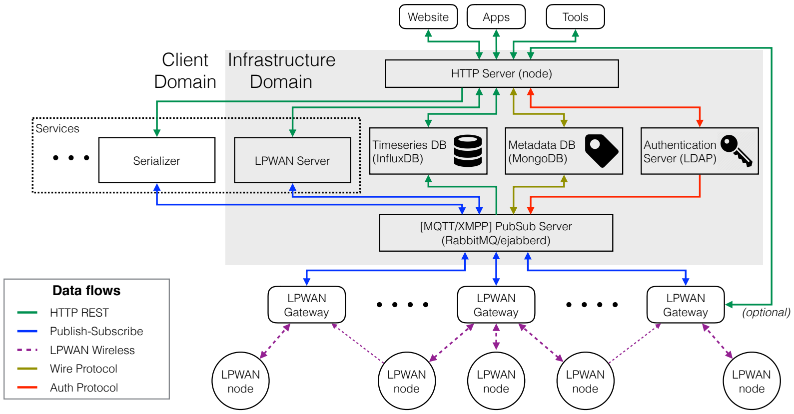


Fig. 1. System architecture for the OpenChirp network

server, the LoRa community often refers to the system as having a “MAC-in-the-Cloud” design. Part of our motivation for using LoRaWAN lies in its open nature and flexibility of implementation.

OpenChirp builds upon LoRaWAN by adding a user management framework, application interface and a set of core services for performing data serialization (converting over-the-air binary data into a typed form with a schema), meta-data management and time series data storage. This is analogous to layers five through seven of the OSI stack (session, presentation and application) with the addition of an Infrastructure-as-a-Service (IaaS) layer on top that gives developers management and monitoring tools. In the purest sense, a LoRaWAN server is responsible for delivering binary blobs to an application while OpenChirp provides structured data with supporting meta-information and services like a web interface and storage. All system configurations are carried out using a REST interface while devices that require more direct access to data like gateways or processing agents communicate using a Publish-Subscribe layer. Since LoRa radios operate in the ISM-band, one of our goals is to both simplify the users ability to add new LoRaWAN gateways to a system as well as optimize overall performance across communities that want to share bandwidth and coverage. Unlike modern cellular networks, the devices in a community-driven network are managed by the users and may be unreliable. This becomes a challenge in terms of network optimization. Much like with peer-to-peer networking services (e.g. BitTorrent), we need mechanisms that can evaluate reliability and enforce fairness.

Our main contributions in this paper are the architecture of the OpenChirp network, the introduction of an open-source low-cost low-power hardware reference called the LoRaBug with an analysis of its energy consumption, range and building penetration. We also discuss the challenges of large-scale LPWAN deployments.

II. Related Work

Recent LPWAN technology can provide robust, low-power and low-cost connectivity to a large number of devices [1]. In this section we describe competing technologies and other frameworks in the LPWAN space.

A. *LPWAN Technologies*

Sigfox [2] provides an ultra-narrow-band LPWAN built on IEEE 802.15.4 radios. It operates in the unlicensed 868 MHz and 915 MHz spectrum in Europe and the US respectively. Devices can communicate over long ranges (tens of kilometers) in a star topology, using low data rates (100 bits/s) and narrow bandwidth (100 Hz/channel), which enables extremely low-power communication. Sigfox deploy and operate gateways, functioning similar to cellular operators. Unlike LoRaWAN, the network layer is proprietary.

LTE Cat-M1 or enhancements for machine type communication (eMTC) is the 3GPP adaptation of LTE for LPWAN [3]. For low cost and energy reduction, devices operate on lower bandwidths (1.4 MHz/channel) with low data rates ($<$1 Mbps) and half-duplex communications. Regular LTE functionality like mobility and hand-off are still supported. eMTC additionally provides power-saving modes and extended discontinuous receptions that allows devices to enter extended periods of deep-sleep without losing their network registrations. These networks function in the licensed LTE spectrum owned by cellular operators, which will be regulated and subject to service contracts.

Narrowband IoT (NB-IoT) [3] is similar to LTE-eMTC but operates at even lower bandwidths (180 kHz/channel) and lower data rates (20 kbps) in the licensed LTE spectrum. Mobility is sacrificed in favor of better indoor coverage and support for larger number of devices. Like eMTC, it would be managed by cellular operators with expected costs and regulations on access to this network.

Due to the extensive interest in LPWANs, a number of other technologies are also already deployed and in development [4]. These are either closed protocols or are yet to gain wide adoption.

B. *LoRaWAN-based Networks*

We describe two examples out of a number of LoRaWANs currently deployed around the world. The Things Network [5] is a community-driven LPWAN initiative started in Europe. They provide gateways and end-devices along with online infrastructure for device management and communication. Symphony Link [6] is a similar network promoted by Link Labs which added listen-before-talk functionality to LoRaWAN as well as a few other non-standard enhancements to improve bandwidth utilization.

III. OpenChirp Architecture

This section describes the architecture of the OpenChirp network as shown in Figure 1. Broadly, OpenChirp maintains the infrastructure domain while elements in the client domain are externally managed.

A. Application Programming Interface (API)

External devices communicate with the OpenChirp network through two interfaces: (1) HTTP REST and (2) Publish-Subscribe (Pub-Sub). Client websites, mobile applications, management tools, etc. interface through an HTTP REST interface. The REST interface provides easy management of devices and their properties (location, metadata, functionality etc) as well as access to device time-series data. HTTP operations are managed by a server implemented in *node*. Separating the OpenChirp API from the internal implementation of various services helps us create a modular architecture that also allows us to experiment with various components of the infrastructure.

B. Publish-Subscribe Dataflows

Heavily-constrained end-nodes with sensors are the primary producers of information in most IoT deployments. Publish-Subscribe (Pub-Sub) architectures help decouple the producers and consumers of information in terms of timing and availability. We often see multiple consumers subscribe to the same produced data. Finally, relatively resource-heavy operations like access control are managed by more capable machines in the infrastructure rather than in the end-nodes. LoRaWAN gateways communicate with OpenChirp using XMPP or MQTT Pub-Sub flows. Various internal dataflows (e.g. between databases and services) are also implemented using Pub-Sub. *ejabberd* and *RabbitMQ* implement the XMPP and MQTT servers respectively to support this.

C. Services

In the OpenChirp infrastructure, *services* provide additional features through server hosted software modules. We provide a framework that services can use if they wish to be notified about new devices, subscribe to and process their data feeds. Some examples of additional functionality provided by services is data serialization/de-serialization and LoRaWAN network management described below.

1) Data Serialization: A node can transfer limited data (tens of bytes per packet) over a LoRa connection due to a combination of communication restrictions and energy constraints. Data serialization gives us a flexible format to transfer various data types inside a single message structure. There are two observations with serialization: (1) the size for preregistered serialized messages is much smaller than if the same data were to be sent over raw key-value pairs and (2) existing serialization tools allow for faster processing and also enable static checking on serialized data. For the serialization service, OpenChirp uses a simplified version of Google's Protocol Buffer [7], which can efficiently represent datatypes. When a new node is registered on the network, its serialization format is registered with the service. The service can then encode and decode data exchanged with the node.

2) LPWAN Server: The LPWAN server is responsible for processing, decrypting and managing LoRa communications in the OpenChirp network. We currently use the open-source LoRa server project [8]. Similar to other servers, it is responsible for MAC decisions like selection of the best downlink gateway, data rates and power levels for messages. Since our objective in OpenChirp is to provide structured data and meta-data, our LPWAN server additionally handles device join requests and also manages encryption. When a new end-node is registered on the OpenChirp network, its relevant meta-data and encryption keys are made available to the LPWAN server.

D. Timeseries and Meta-Data Storage

A common application of IoT is identifying and acting on trends in the environment which requires data history. OpenChirp thus provides a time-series database (using *InfluxDB*) that stores all data to and from end-devices. Applications and services can thus access historical data on-demand for a given time-interval in an efficient manner. This is accessible through our common REST API.

Some end-node and gateway properties like location, device type, capabilities, sensor sampling rates, closest gateway, etc. provide meaning and context to their data. These properties are stored as device metadata in an independent NoSQL (*MongoDB*) database which also maintains access-control lists to regulate access to/modification of device data and meta-data. An LDAP authentication server is used to authenticate users that use the OpenChirp network. In our current deployment, students on campus can register and deploy their own devices with access control. If desired, they can share access with other account holders.

E. LPWAN Gateways

Gateways are responsible for converting raw LoRa messages into the Pub-Sub flows used by OpenChirp. Gateways can be owned and deployed by anyone. Thus, we do not store device-specific encryption keys locally on the gateway in our current deployment. The gateway is powered by a Raspberry Pi 3 connected to a custom LoRaWAN concentrator over SPI[1] and connects to the internet over WiFi or Ethernet. Power-over-Ethernet (PoE) simplifies deployment of the gateways. We also include an RTL software-defined radio for future exploration of whitespaces and listen-before-talk (LBT) functionality as well as a GPS radio for localization and time-synchronization. For extended use in rough outdoor environments, we hardened the deployed hardware (weather-resistant design) and software (watchdog resets). The gateway communicates with the OpenChirp network over a secure MQTT connection.

---

[1] Early LoRa reference designs had a USB-serial interface that dropped data

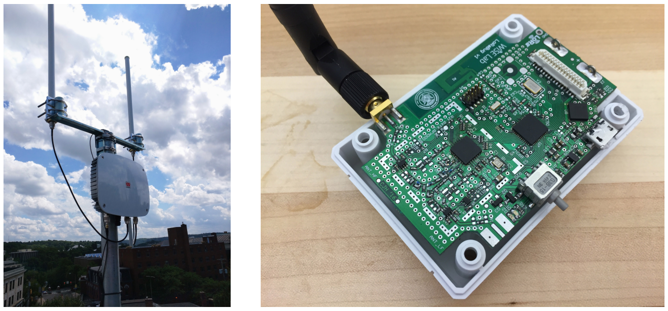


Fig. 2. Photo of an OpenChirp gateway (left) and a LoRaBug node (right)

F. Network Coverage and Signal Penetration

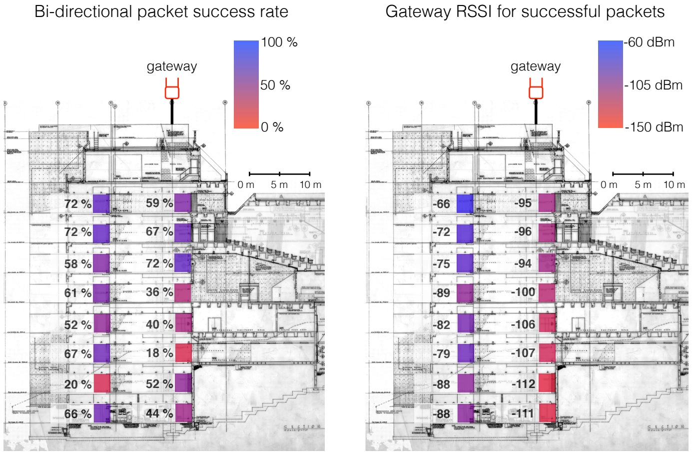


Fig. 3. RF signal penetration experiments performed in a large poured-concrete building on campus. (left) shows the success rate for bi-directional packet exchange between end-node and gateway and (right) shows the RSSI at the gateway for successful transfers.

A major objective of the OpenChirp network is to be able to serve CMU's campus with a minimal constellation of gateways. This requires coverage of the complete geographical area as well as signal penetration inside buildings. After installing only four gateways on the roof of campus buildings, we perform a set of coverage tests. The tests are performed with a LoRa end-node configured for uplink communications with 125 kHz channel bandwidth, data rate of 980 bits/s, spreading factor of 10 and coding rate of $4/5$. Downlink communications from the gateway used 500 kHz channels at 3900 bits/s. Figure 4 shows the coverage heatmap based on the average received signal strength indicator (RSSI) of ~ 12 messages sent from each location. Though some regions may not be covered using one gateway (due to shadowing, attenuation, etc.), a combination of four gateways can successfully cover all major campus regions. Figure 3 shows the signal penetration across multiple floors of a large 250,000 sq.ft. 9-story poured concrete building with a single gateway located on the roof. The packet success rate on the left is computed based on the number of complete bi-directional transfers (~ 60 points in each left corridor, ~ 15 points in each right corridor). The image on the right shows the gateway RSSI of successful transfers.

IV. LoRaBug Hardware Platform

We developed an open-source, low-cost, low-power, and extensible LPWAN end-node hardware platform named LoRaBug [9] shown in Figure 2b. The main motivations for the development of this platform are (1) ease-of-use in terms of registration, (2) expandability and (3) a well profiled reference firmware stack that can maintain low-power consumption. We envision OpenChirp simplifying deployment through a combination of BLE configuration of end-devices and a simple web-portal for registrations.

The LoRaBug hardware is housed in a small plastic enclosure that accommodates two AA batteries. The LoRaBug itself provides processing and communication while *expansion modules* provide the sensing and actuation functionality. These are attachable daughter boards containing application specific sensors and actuators. For example, we use an expansion module that has passive-infrared, temperature, humidity, sound, acceleration, and light sensors to monitor rooms in campus buildings. We discuss energy consumption in Section IV-B. The LoRaBug is powered by a Texas Instruments CC2650 microcontroller (MCU) with integrated 2.4 GHz IEEE 802.15.4 and Bluetooth Low-Energy (BLE) radios. It communicates to LoRa networks through a Semtech SX1276 LoRa radio. The node can be augmented with expansion modules for a variety of applications (e.g. environmental sensing, GPS localization and actuation). In addition to typical sleep states, the MCU has an ultra low-power sensor co-processor for sensor sampling and data aggregation, and a cryptographic accelerator that enhances the performance of security functions and reduces code-size.

A. Firmware

The LoRaBUG firmware is built on top of the open-source TI-RTOS. Based on the application, the firmware can be configured from a minimal multitasking kernel to a complete network-enabled environment supporting low-energy operation. The LoRaBUG connects to networks such as OpenChirp (as class A or B LoRaWAN device) using the IBM LMiC library [10]. LMiC supports both over-the-air activation (network parameters shared by joining the network) and activation by personalization (network parameters directly stored in device). Mobile devices can interact with the LoRaBug using the MCU's integrated BLE radio that allows for easy configurations and communication. The BLE stack is a TI-RTOS extension and the firmware can be created with (using 13.9 KB Flash and 6.2 KB free SRAM) or without it (using 75.4 KB Flash and 10.6 KB free SRAM). Over-the-Air (OTA) updates may be performed if the flash space is partitioned into two parts for the running firmware and its update. Due to the limited size of available flash, we recommend adding external storage for OTA updates on the sensor expansion modules.

B. Energy Consumption

Both our MCU and LoRa radio have multiple sleep and function states that consume varying amounts of power. In Figure 5a we look at the current consumption of these devices

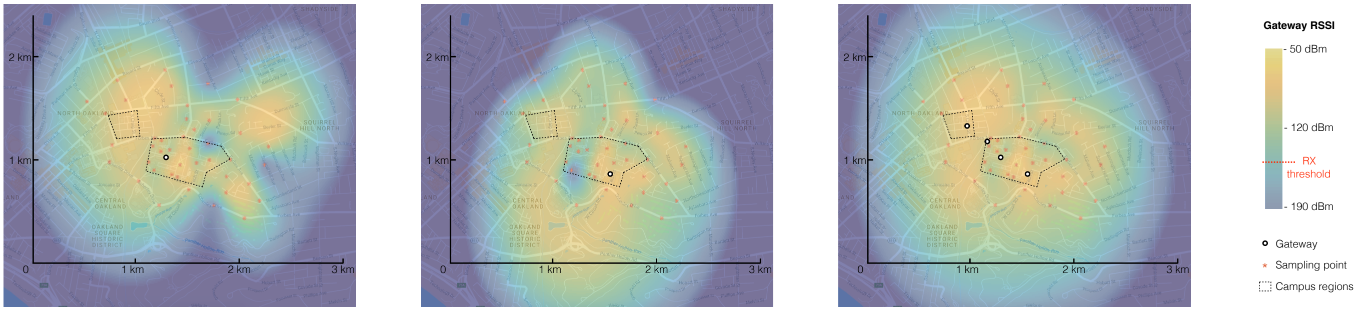


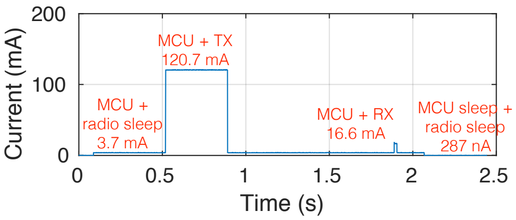
Fig. 4. Network coverage in and around CMU campus. (left) Wean Hall gateway, (middle) GSIA gateway and (right) combination of all gateways.

while sending out 8 bytes of data and receiving an acknowledgment with radio parameters similar to Section III-F. Based on a simple power model, we estimate the lifetime of these devices in Figure 5b while operating on two 2000 mAH AA batteries (we make a conservative estimate of 60 % usable energy and maximum shelf life of 10 years). Thus, with proper duty-cycling, a LoRaBug can function and communicate for multiple years on simple batteries.

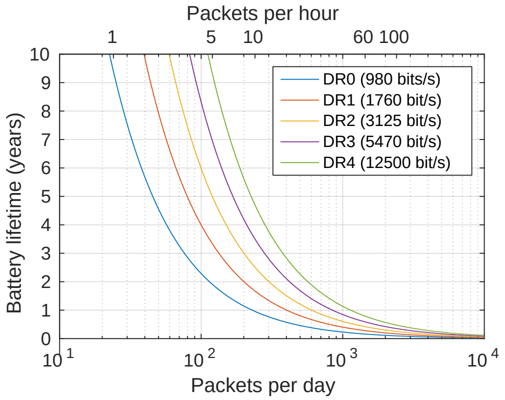
During the development of the LoRaBug, we found that the Semtech reference design for end-nodes [11] cannot shutoff its RF switches. This results in a constant draw of 20 μA even while the rest of the device is in deep-sleep. This error severely impacts battery lifetime of LoRa end-nodes but is easily correctable (as implemented in the LoRaBug).

V. CHALLENGES

In this section, we discuss open problems in the LPWAN space and properties like localization, scalability, security, privacy and efficient spectrum usage.



(a) LoRaBug current consumption over time for transmitting a packet and then checking for an ACK from the gateway.



(b) Lifetime of a LoRaBug powered by two AA batteries at various operating points based on a measured energy profile.

Fig. 5.

A. *Localization*

Traditional solutions for loaclization like GPS can provide sufficient accuracy, but are power-hungry, expensive and primarily work outdoors with an open sky view. It is often too restrictive for modern IoT deployments that are heavily cost and resource constrained or reside indoors. This has given rise to schemes based on beacon-proximity, time-of-flight (ToF) and time-difference-of-arrival (TDoA) of wireless messages. Beacon-proximity schemes require a large infrastructure of low-range RF beacons, which is difficult for campus-wide deployment.

Gateways play an important role in the RF localization of end nodes, particularly for timestamping wireless messages for ToF and TDoA schemes. However, current LoRaWAN hardware and software implementations limit timestamp resolution to 1 μsec. This limits localization accuracy to worse than 300 m, which is often not sufficient. A practical localization system for very-low power wireless nodes is still an open research problem. We believe systems will need to utilize out-of-band signals or perform channel stitching to improve ToF resolution. They could also use RSSI fingerprinting approaches, especially through crowd-sourced mapping.

B. *Scalability*

Being an open community-driven network, we want gateways and end-devices on OpenChirp to be independently manageable by their owners. This requires mechanisms such that independent setups can coordinate in the network (to share time-slots, frequency lists, user lists, etc.). LoRaWAN uses the MAC-in-the-cloud concept for data downlinks which can cause multiple issues (high latency, overload, reliability, etc.) that must be solved by developing a distributed version of the LoRaWAN server. The estimates for the number of nodes supported per gateway vary from 120 [12] to commercial estimates of 10000. However, many commercial estimates assume the use of adaptive data-rates (ADR) which is currently not supported and must be added to software stacks. This will require a detailed analysis of LoRa communication to develop acceptable models for ADR.

C. *Security and Privacy*

A number of factors make LPWANs vulnerable to attack. LPWANs contain a large number of devices spread over physically large areas and managed by different entities.

Device hardware (and correspondingly firmware) can thus be directly accessed and compromised. End-nodes are low-cost and have limited capabilities, which prevents them from using stronger but more resource-intensive security techniques. IoT-focussed MCUs like the CC2650 on the LoRaBug address this problem by providing dedicated crypto-coprocessors. However care must be taken, since recent attacks [13] have exploited bad initial configuration and setup of devices. The LoRaBug can be configured to connect to the OpenChirp network using a BLE connection, which helps, but by no means solves this issue. End-devices vary in hardware and capabilities, which makes it difficult to deploy generic defenses. OpenChirp and LoRaWAN use separate keys for application and network functions to mitigate problems from compromised keys. BLE over-the-air updates on the LoRaBug would be able to address the problem of firmware, configuration and key updates.

As IoT devices can interact with entities in the physical world, it is also essential to extend the concepts of net-neutrality (users traffic must not be unfairly classified/treated) and accountability (help identify the source of events) to LPWAN networks. We believe the appropriate usage of access-control and network storage would help with these issues.

Though we attempted to address many of the security and privacy concerns individually in our architecture and hardware design, a well-structured and proven security and privacy framework for LPWANs and its practical implementation is still an open challenge.

D. Spectrum Efficiency

Many LPWANs operate in the unlicensed but limited ISM spectrum. We can envision two major directions for improvements in spectrum usage: (1) effective use of ISM spectrum and (2) use of non-ISM unlicensed spectrum e.g. whitespaces.

Current LoRaWAN gateway chipsets are designed to listen on 9 channels simultaneously (compatible with channel frequency lists in EU regulations). US regulations require high-power transmissions to hop over more channels. The first challenge is to develop protocols for current gateway chipsets that can use all 72 channels in the US specifications [14]. A second challenge is to develop better listen-before-talk MAC protocols (similar to [6]) to minimize interference from uncoordinated nodes and LPWAN networks.

Many regions around the world allow unlicensed usage of UHF and VHF spectrum when the spectrum is not being used [15], [16]. Current LoRaWAN end-nodes like the LoRaBug can already communicate on frequencies between 137-1020 MHz, which covers a large portion of the whitespace spectrum. LPWAN communications over whitespaces could significantly reduce contention on the ISM band. However, this would require better time-synchronization, infrastructure for disseminating channel information and listen-before-talk functionality.

VI. CONCLUSION

In this paper, we presented the design and early results of OpenChirp, which is an LPWAN architecture built on top of LoRa and LoRaWAN. OpenChirp is an evolving research platform designed to enable collaborative and communal wide-area networking for telemetry. We believe open LPWAN networks have the potential to unlock a plethora of creative ideas that are currently either power or cost limited by existing wireless technology. The OpenChirp architecture demonstrates a proof-of-concept system deployed at Carnegie Mellon University that shows the feasibility of low-powered sensing devices at scale. We demonstrated that a few well positioned gateways can easily cover an entire college campus and that low-cost nodes can be designed and deployed to run on batteries for many years. As future work, we will begin addressing many of the challenges outlined within this paper.

ACKNOWLEDGMENT

This work was supported in part by the Bosch Research and Technology Center (RTC) and TerraSwarm, one of six centers of STARnet, a Semiconductor Research Corporation program sponsored by MARCO and DARPA. We would also like to thank Orne Brocaar for providing an amazing open-source LoRaWAN server, and Link Labs Inc. for providing hardware and firmware support while building OpenChirp gateways.

REFERENCES

[1] V. Atanasovski and A. Leon-Garcia, *Future Access Enablers for Ubiquitous and Intelligent Infrastructures*. Springer, 2015. [Online]. Available: http://link.springer.com/10.1007/978-3-319-27072-2

[2] "Sigfox," accessed Jan 10, 2017. [Online]. Available: https://www.sigfox.com/

[3] GSM Association, "3GPP Low Power Wide Area Technologies (White Paper)," 2016.

[4] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low Power Wide Area Networks: A Survey," pp. 1–15, jun 2016. [Online]. Available: http://arxiv.org/abs/1606.07360

[5] "The things network," accessed Jan 10, 2017. [Online]. Available: https://www.thethingsnetwork.org/

[6] "Symphony link — link labs," accessed Jan 10, 2017. [Online]. Available: https://www.link-labs.com/symphony/

[7] "Protocol buffers - google developers." [Online]. Available: https://developers.google.com/protocol-buffers/

[8] O. Brocaar, "Lora server - open-source lorawan server," accessed Jan 10, 2017. [Online]. Available: https://docs.loraserver.io/loraserver/

[9] "Lorabug repository," accessed Jan 10, 2017. [Online]. Available: https://github.com/OpenChirp/LoRaBug

[10] "Lora wan in c - ibm," accessed Jan 10, 2017. [Online]. Available: https://www.research.ibm.com/labs/zurich/ics/lrsc/lmic.html

[11] *137 MHz to 1020 MHz Low Power Long Range Transceiver*, Semtech Corporation, 3 2015, rev. 4.

[12] M. Bor, U. Roedig, T. Voigt, and J. M. Alonso, "Do lora low-power wide-area networks scale?" in *Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*. New York, NY, USA: ACM, 2016, pp. 59–67.

[13] D. Etherington and K. Conger, "Large ddos attacks cause outages at twitter, spotify, and other sites." [Online]. Available: https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/

[14] N. Sornin, M. Luis, T. Eirich, T. Kramp, and O. Hersent, "Lorawan specifications," *LoRa Alliance*, 2015.

[15] FCC, "Second Report and Order and Memorandum Opinion and Order," *Tech. Rep.*, 2010. [Online]. Available: http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-260A1.pdf

[16] X. Feng, J. Zhang, and Q. Zhang, "Database-assisted multi-ap network on tv white spaces: Architecture, spectrum allocation and ap discovery," in *New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2011 IEEE Symposium on*. IEEE, 2011, pp. 265–276.